(12) UK Patent Application (19) GB (11) 2 214 673(13)A

(43) Date of A publication 06.09.1989

(21) Application No 8901994.7

(22) Date of filing 30.01.1989

(30) Priority data
(31) 8802038 (32) 29.01.1988 (33) GB

(71) Applicant
Texas Instruments Limited

(Incorporated in the United Kingdom)

Manton Lane, Bedford, MK41 7PA, United Kingdom

(72) Inventors
Peter James Vinson
David Trevor Cutler
Christopher Thurson Black

(74) Agent and/or Address for Service
Abel & Imray, Northumberland House,
303-306 High Holborn, London, WC1V 7LH,
United Kingdom

(51) INT CL⁴
G06F 11/10

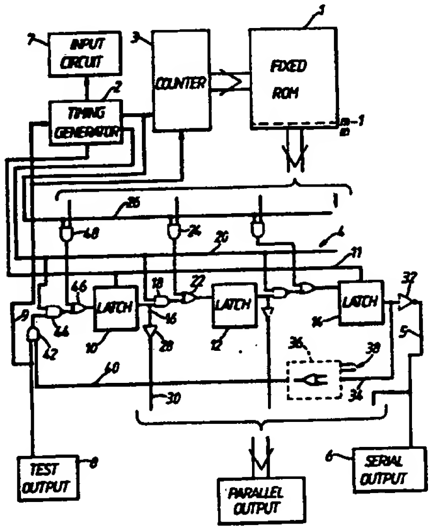
(52) UK CL (Edition J)
G4A AFMF

(56) Documents cited
GB 1597043 A WO 85/03785 A US 4730320 A
US 4689792 A US 4488300 A

(58) Field of search
UK CL (Edition J) G4A AAP AEN AFMF AFMR
AFMW
INT CL⁴ G06F

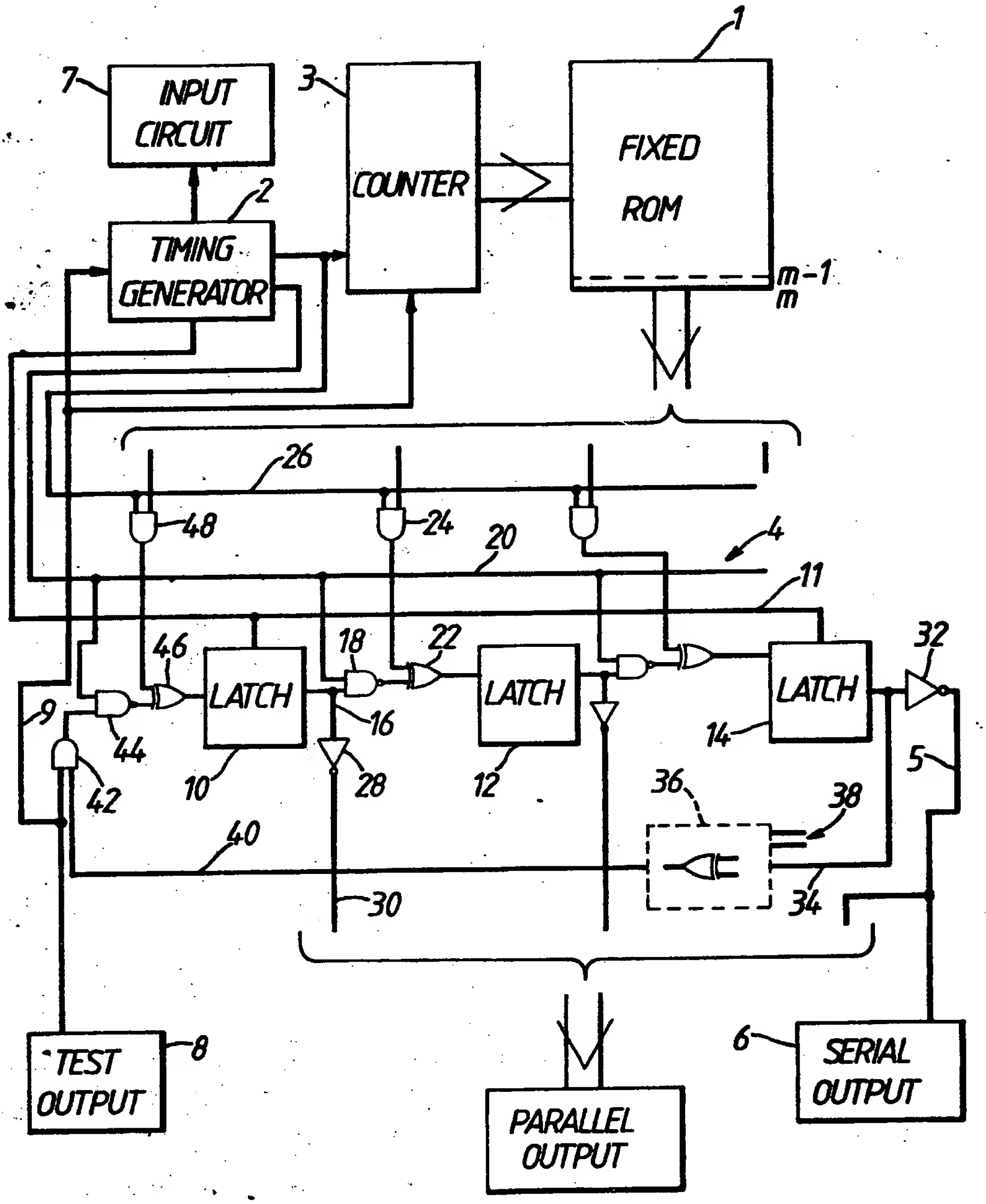
(54) Electronic control device for producing a particular code group of digits when energizsed.

(57) An intergrated circuit includes a read-only memory 1 storing a particular code group of digits which it produces as an output when energised. The memory also stores a test group of digits which can be output in conjunction with the particular code group and logically combined with it using a predetermined signature generation process by means included in the integrated circuit to produce a signature group of digits. The test group of digits is so chosen taking into account the particular code group of digits that the signature group of digits is the same for different particular code groups, so that the correct operation of the integrated circuit in producing different particular code groups of digits can be tested by comparing the signature code group with a single reference group.



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

GB 2 214 673 A


1
7
INPUT CIRCUIT
3
COUNTER
FIXED ROM
2
TIMING GENERATOR
m-1
m
26
48
24
20
4
11
46
18
22
LATCH
LATCH
LATCH
32
9
44
16
14
42
10
28
12
5
36
38
40
34
30
8
TEST OUTPUT
PARALLEL OUTPUT
6
SERIAL OUTPUT

Electronic Control Device for Producing a Particular Code Group of Digits when Energised

This invention relates to an electronic control device for producing a particular code group of digits when energised. The energisation may occur when the device is interrogated by a host device.

There are many security and identification applications for devices which on interrogation produce a particular code group to a host device which responds to that group in a predetermined manner. One such application is as an electronic key or security pass when the host device releases a lock on receiving the correct coded pulse group or one of a plurality of different coded pulse groups which it can accept. The device may be powered by a battery or it may derive its entire energisation from the host device through electrical connections or electromagnetic radiation from the host device. The communication from the device to the host device may be through connections or via electromagnetic or ultrasonic radiation.

Another application for the devices is for identifying individual animals of a herd so that special feeding requirements or medication can be supplied, the device being attached to the animals in a suitable manner.

Since many of the uses of such devices are in security applications, it is important that the coded digit group is fixed in the devicei.e. stored so that it cannot be changed. Most conveniently, the coded group is stored in a read only memory, but it must be such a memory that, once it is programmed, cannot be altered. Certain types of ROM for example, fuse-link, EPROM and EEPROM permit the stored codes to be altered which would compromise the security and would therefore be unsuitable for use in the device. The preferred form of construction of read-only memories is as integrated circuits because once the memory has been manufactured its small size makes it difficult to interfere with and it is also relatively inexpensive to make.

It is important to be able to test the integrated circuit during its production because a device incorporating an integrated circuit which owing to some defect in its manufacture causes the device to produce the wrong output code or none at all when interrogated would be useless. On the other hand, security and identification applications call for devices with many different code groups and these must be reliably produced. In order to test the devices, the test must take account of the code group which is supposed to be stored in it and ensure that the correct output pulses are produced. This means that it is necessary to keep track of the devices after the programming of the ROM has been done during the final processes of its manufacture to ensure that the correct test is applied to the device.

It is an object of the present invention to facilitate the testing of such an electronic control device.

According to the present invention, there is provided an electronic control device for producing a particular code group of digits when energised, the device having a read-only memory for storing the particular code group of digits, reading means for reading the digits from the memory, output means at which output signals are produced in response to signals read from the memory by the reading means and input means which when energised causes the reading means to read the code group only from the memory and corresponding output signals to be produced at the output means wherein the memory also stores a test group of digits which is so related to the code group of digits that the combination of the code group and the test group produces a fixed signature group when subjected to a predetermined signature generation process, and the device includes a test input which when energised causes the reading means to read both the particular code group and the test group from the memory and activates a logical means responding to the combination of the particular code group and the test group together to generate a signature group of digits for the combination by the predetermined signature generation process.

The digits may be binary digits (bits).

The integrated circuit may also include the input means and the logical means.

The device may include a shift register into which several digits can be transferred in parallel from the memory and from which the stored digits can be output in serial form.

The signature group may be generated by applying the required logical operation to the digits read from the memory in series using a shift register to recirculate digits read from the memory earlier for combining them with digits read later from the memory.

The digits may be read from the memory a word at a time in parallel and the logical operations required to perform the signature generation applied in parallel to the digits of a word. The resulting signature group may be stored in a shift register and output in serial form.

According to a second aspect of the present invention there is provided a method of testing an integrated circuit containing a read-only memory in which the memory contains a multi-word digital code group, the method comprising providing in the memory an additional word forming a test group which is such that the signature generated by the code group and test group together is a particular signature word when subjected to a predetermined signature generation process, reading the data from the memory, subjecting the data read therefrom to the predetermined signature generation process and comparing the signature so produced with a reference word.

One example of a device according to the invention will now be described with reference to the single figure of the accompanying drawing which shows it in block schematic form.

Referring to the drawing, a read only memory 1 having m rows each containing n digits is provided to store the particular code group and a test group of digits, the code group occupying m-1 rows and the test group the final row. The digits are binary digits and will be referred to as bits. Preferably there are at least ten bits in each row.

A timing generator 2 is provided to drive a counter 3 connected to address the m rows of the memory 1 in sequence. The counter 3 has two modes of operation, in the first of which it addresses only the first m-1 rows of the memory and in the second of which it addresses all m rows of the memory. A shift register and signature generator unit 4 is connected to receive the n bit words from the memory 1 in parallel as they are produced in response to the addressing of the rows by the counter 3. The timing generator 2 is also connected to the unit 4 applying an enable signal to a conductor 20 and pulses to a conductor 11 at n times the rate at which it applies signals to the counter 3 so as to cause the n bit words to be stepped out serially via a conductor 5 to a serial output circuit 6.

When the device is required to produce the stored code group from the memory 1 as a serial output through the circuit 6, an input signal is supplied to an input circuit 7 which then applies a starting signal to the generator 2. The counter 3 is then caused to apply an input to the first row of memory 1 to transfer the n bits stored in that row into the unit 4. The timing generator 2 then applies n shift pulses to the unit 4 to transfer the n bits stored in the unit serially into the output circuit 6. When this is completed, the generator 2 applies a pulse to the counter 3 causing it to address the second row of memory 1 and transfer the n bit word from that row into the unit 4 for serial transfer to the circuit 6. This process continues until the m-1th row of the memory 1, when the counter 3 returns to the first row of the memory to repeat the cycle, the whole of the particular code group stored in the memory having been transferred to the output circuit 6 through the unit 4. Alternatively, the counter 3 may be arranged to stop when it reaches the m-1th row so that the code group is produced only once. The mth row of the memory 1 contains the test group of digits which is not output to the unit 4 in the normal operation of the device.

A parallel output, a word at a time, could alternatively be produced directly from the stages of the unit 4.

When it is required to test the device to ensure that it produces the correct particular code group output when interrogated, a test input 8 is energised and a signal is applied via a conductor 9 to modify the operation of the counter 3 causing it to read the mth row of the memory 1 after the first m-1 rows have been read. The signal on the conductor 9 is also applied to the timing generator 2 to switch its outputs so that the shift register and signature generator unit 4 performs a signature generation operation on the m words output from the memory 1.

The shift register and signature generator unit 4 contains n latches 10, 12, 14, i.e. equal in number to the bits of a word stored in the memory 1. Each latch is connected to a conductor 11 which is connected to receive from the timing generator 2 at appropriate times pulses enabling the latches to adopt the states represented by the respective input signals to the latches. The circuitry interconnecting an adjacent pair of latches is the same in each case, and that connecting the latch 10 to the latch 12 will now be described. An output from the latch 10 representing the stored bit appears on conductor 16 and is applied as an input to a 2-input NAND-gate 18, the second input of which is connected to the conductor 20. The output of the gate 18 is connected to an input of an exclusive-OR-gate (XOR-gate) 22. The second of the n output conductors of the memory 1 is connected to an input of a 2-input AND-gate 24, the second input of which is connected to a conductor 26 and the output of which is connected to the second input of the XOR-gate 22. The output of the gate 22 is connected to the input of the latch 12 which registers the state of that output at the next pulse on the conductor 11.

When operating as a shift register the unit 4 receives a shift enable signal on the conductor 20 as well as the pulses on the conductor 11 from the timing generator 2. There are no signals on the conductor 26 at this time so that the AND-gate 24 is closed and produces a "0" output. Because the NAND-gate 18 is opened by the enable signal on the conductor 20 there appears at the output of the NAND-gate 18 a signal representing the bit stored in the latch 10 in an upright form and this signal passes through the XOR-gate 22 and is applied to store the bit in the latch 12 at the next pulse on the conductor 11.

Each time the counter 3 receives a signal from the timing generator 2 and consequently reads a word from the memory 1, the signal is also applied to the conductor 26 so enabling the AND-gate 24 to pass the signal representing the corresponding bit of the word read from the memory to the XOR-gate 22. If no enable signal is applied to the conductor 20 at this time the output of the gate 18 is a "1" causing the XOR-gate 22 to act as inverter on the bit from the memory 1 so that the complement of that bit is stored in the latch 12 at the next pulse on the conductor 11.

Because the bits stored in the latches 10, 12, 14 are the complements of those read from the memory 1 an inverter 28 is provided connected to the output of the latch 10 so that the bit is restored to upright form on a conductor 30 as part of the parallel output of the unit 4. An inverter 32 performs the same function for the latch 14 so that the serial output of the unit 4 is also in upright form.

The unit 4 contains some circuitry additional to that required by a shift register so that it performs signature generation. The output of the latch 14 is fed back via a conductor 34 to a circuit 36 containing at least one XOR-gate. The circuit 36 combines the outputs of at least two stages of the unit 4 using XOR-gates connected in series, the connections to other stages than the last being represented by the lines 38. The connections to other stages depend on n, the number of stages in the shift register, and examples of the connection arrangements may be found in papers discussing signature generation, one such paper being entitled "Built-in Logic Block Observation Techniques" by B. Konemann, J. Mucha and G. Zweihoff published in The Digest of Papers from the 1979 International Test Conference, pages 37 to 41.

The output of the circuit 36 appears on a conductor 40 and is applied to an input of an AND-gate 42 controlled by the signal applied to the test input 8. The output of the gate 42 is connected to an input of a NAND-gate 44, the other input of which is connected to the conductor 20. The output of the gate 44 is applied to an input of an XOR-gate 46 which receives the first bit of a word from the memory 1 via an AND-gate 48 controlled by the signal on the conductor 26. The output of the XOR-gate 46 is connected to the input of the latch 10. It should be noted that the gates 44, 46 and 48 form a circuit of the same design as that formed by the gates 18, 22 and 24 between latches 10 and 12, and that both circuits operate in the same way.

As mentioned above, when the device is to be tested a signal is applied to the test input 8. This signal causes the counter 3 to count up to m instead of m-1. It also is applied to the timing generator 2 causing the generator 2 to apply signals to the conductors 20 and 26 and pulses to the conductor 11 simultaneously. The gate 42 is also opened by the test input signal.

The application of signals simultaneously to the conductors 20 and 26 causes the unit 4 to perform signature generation, because a word is read from the memory 1 at the same time as outputs representing the bits already stored in the latches 10, 12, 14 are produced. The XOR-gates connected to the inputs to the latches receive two input bits at the same time, one from the memory 1 and one from the preceding latch, and form the exclusive-OR function of them which is applied to the input of the following latch to be stored there in response to a pulse on the conductor 11. In addition, the bit from the last latch of the register is fed back via the circuit 36 to the input of the register, the circuit 36 combining the bit from the last latch with the bits from other latches as explained above. After all m words have been read from the memory 1 into the unit 4 there remains in the latches an n bit word termed the signature of the multi-word data stored in the memory 1, and this is then shifted out to the serial output circuit 6 using the unit 4 as a shift register.

The mth word stored in the memory 1 is so chosen, taking into account words 1 to m-1, that the signature obtained is a predetermined n bit word which is the same for all sets of m words despite the fact that words 1 to m-1 differ. One such group of bits is 1010...01. Preferably, the bits of this group are not all the same so that the operation of the unit 4 and the output circuits are also checked by the test. The group should contain a sufficiently large number of bits to ensure that the test will detect most errors which could occur in the coded data; this means that n should be at least 10 and is preferably larger.

The process of combining selectively the bits of a long sequence of bits using one or more exclusive-OR gates results in the production of a shorter sequence termed its signature. As described above, the process is performed in parallel n bits at a time on m x n bits to produce a signature of n bits. Since the test group causes the resulting signature to be of a predetermined form, it could be referred to as the signature complement of the code group of (m-1)n bits.

An advantage of using signature generation for deriving a small group of bits characteristic of a larger group of bits is that it is simple to implement and requires only a small area of semiconductor material for the fabrication of the circuit required.

For many applications it is required that each device has a different code group of bits. There are many ways in which this can be done, for example the code group may be arranged to consist of a batch number and a sequence number within the batch or a coded version of the date and time of manufacture of the memory. Conveniently, the generation of the code groups may be performed by a computer which also controls the manufacture of the memory and calculates the required test word as the memory is being made, ready to store it in the last row of the memory.

For applications in which it is important that the information stored in the read-only memory should not be alterable, that is to say where security is a factor in the use of the device, the memory may be of the type in which connections to the storage cells of the memory are selectively cut using an electron beam or a laser beam. This cutting is most conveniently done during the manufacture of the device with the machine controlled by a computer.

A device according to the invention may be powered by a local battery or other power supply so that it can be switched on or triggered to start the production of the output signals representing the code group. Alternatively the device may be powered remotely and/may include means for deriving energy for its operation from electromagnetic radiation transmitted to it.

The output signals representing the code group may be applied directly to a host device or may be transmitted to the host device as modulated electromagnetic signals or ultrasonically.

The testing of the device may be arranged to include tests of the power supply and output signal transmission as well as the correct functioning of the memory and the shift register.

Possible applications for the device include

identification tags for animals, inventory, personnel or samples,
access codes for secure modems,
software keys ("dongles") for computer systems,
motor vehicle door locks,
credit cards,
security passes,
ownership coding of valuables, and
in defence electronics.

CLAIMS:

1. An electronic control device for producing a particular group of digits when energised, the device including a read-only memory for storing the particular code group of digits, reading means for reading the digits from the memory, output means at which are produced output signals in response to signals read from the memory by the reading means and input means which when energised causes the reading means to read the code group only from the memory and corresponding output signals to be produced at the output means, wherein the memory also stores a test group of digits which is so related to the code group of digits that the combination of the code group and the test group produces a fixed signature group when subjected to a predetermined signature generation process, and the device includes a test input which when energised causes the reading means to read both the particular code group and the test group from the memory and activates a logical means responding to the combination of the particular code group and the test group together to generate a signature group of digits for the combination by the predetermined signature generation process.

2. A device according to claim 1 constructed as an integrated circuit.

3. A device according to claim 1 or 2 wherein the read-only memory is a fixed non-erasable memory.

4. A device according to claim 1, 2 or 3 in which the a read-only memory has a plurality of multi-digit word locations addressed by respective outputs from the reading means and producing multi-digit outputs in parallel.

5. A device according to claim 4 further including a shift register to respective stages of which the multi-digit outputs from the read-only memory are applied for storage, means being provided for reading out the stored digits in serial form.

6. A device according to claim 5 wherein logical means for generating the signature group receives the stored digits read out from the shift register in serial form and recirculates them to combine logically digits read from the memory at one time with digits read from the memory at a later time.

7. A device according to claim 5 wherein the logical means for generating the signature group receives the multi-digit parallel output from the memory and applies the signature group in parallel for storage in the shift register.

8. A device according to any preceding claim in which the digits are binary digits.

9. A device according to claim 5 wherein the digits are binary digits and the logical means for generating the signature group comprises a plurality of exclusive-OR gates having their outputs respectively connected to the inputs of the stages of the shift register, the digits of the multi-digit outputs of the memory being respectively applied to first inputs of the exclusive-OR gates, and the inverted outputs of the immediately preceding stages of the shift register being applied to second inputs of the exclusive-OR gates, except for the exclusive-OR gate the output of which is connected to the input of the first stage of the shift register, to the second input of which gate there is applied the output of a circuit containing at least one exclusive-OR gate which combines the output of at least two stages of the shift register.

10. A device according to any preceding claim wherein the test group of digits is so chosen that the signature group of digits produced is a predetermined group of digits.

11. A method of testing an integrated circuit containing a read-only memory in which the memory contains a multi-word digital code group, the method comprising providing in the memory an additional word forming a test group which is such that the signature generated by the code group and test group together is a particular signature word when subjected to a predetermined signature generation process, reading the data from the memory, subjecting the data read therefrom to the predetermined signature generation process and comparing the signature so produced with a reference word.

12. A method according to claim 11 wherein in normal operation of the integrated circuit when the read-only memory is read the digital code group is produced as an output without the test group, and an additional input is required to initiate the signature generation process.

13. A device for producing a particular code group of digits when energised substantially as described herein and as illustrated by the single figure of the accompanying drawing.

14. A method of testing an integrated circuit containing a read-only memory storing a multi-word digital code group, the memory being substantially as described herein and as illustrated by the single figure of the accompanying drawing.

Published 1989 at The Patent Office, State House, 66/71 High Holborn, London WC1R 4TP. Further copies may be obtained from The Patent Office.
Sales Branch, St Mary Cray, Orpington, Kent BR5 3RD. Printed by Multiplex techniques ltd, St Mary Cray, Kent, Con. 1/87